

in cross-agency activities and where component inspectors general may have otherwise faced significant challenges;

(3) because of the cross-agency nature of Federal science and technology activities, Congress created the Office of Science and Technology Policy to coordinate and harmonize among science functions at agencies;

(4) the United States innovation ecosystem, which uses multiple science agencies to invest in research and development, can make it more difficult to identify and remove scientists who violate research integrity principles;

(5) the single agency jurisdiction of an agency inspector general can be a disadvantage with respect to their oversight roles, and opportunities to strengthen the system may exist;

(6) single agency jurisdiction of inspectors general may also make it difficult to harmonize principles and standards for oversight of waste, fraud, and abuse among agencies; and

(7) certain issues of fraud, waste, and abuse in Federal science and technology activities span multiple agencies and are more apparent through cross-agency oversight.

(b) STUDY.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study and submit to Congress a report that—

(1) evaluates the frequency of cases of waste, fraud, or abuse perpetrated across multiple Federal science agencies by an awardee or group of awardees;

(2) evaluates the effectiveness of existing mechanisms to detect waste, fraud, and abuse perpetrated across multiple Federal science agencies by an awardee or group of awardees; and

(3) evaluates options for strengthening detection of waste, fraud, and abuse perpetrated across multiple Federal science agencies by an awardee or group of awardees, including by examining the benefits and drawbacks of—

(A) providing additional support to agency inspectors general with regard to coordinated oversight of Federal and technology grant making investments; and

(B) alternative mechanisms for strengthening prevention and detection of waste, fraud, and abuse across Federal science agencies perpetrated across multiple Federal science agencies by an awardee or group of awardees, such as the establishment of a special inspector general or other mechanisms as the Comptroller General sees fit.

SA 1995. Mr. WYDEN submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title III of division F, add the following:

SEC. 6302. TECHNICAL AND LEGAL SUPPORT FOR ADDRESSING INTELLECTUAL PROPERTY RIGHTS INFRINGEMENT CASES.

(a) IN GENERAL.—The head of any Federal agency may provide support, as requested and appropriate, to United States persons seeking technical, legal, or other support in

addressing intellectual property rights infringement cases regarding the People's Republic of China.

(b) UNITED STATES PERSON DEFINED.—In this section, the term “United States person” means—

(1) a United States citizen or an alien lawfully admitted for permanent residence to the United States; or

(2) an entity organized under the laws of the United States or of any jurisdiction within the United States, including a foreign branch of such an entity.

SA 1996. Mr. WYDEN submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title III of division F, add the following:

SEC. 6302. AUTHORITY OF U.S. CUSTOMS AND BORDER PROTECTION TO CONSOLIDATE, MODIFY, OR REORGANIZE CUSTOMS REVENUE FUNCTIONS.

(a) IN GENERAL.—Section 412 of the Homeland Security Act of 2002 (6 U.S.C. 212(b)) is amended—

(1) in subsection (b)—

(A) in paragraph (1)—

(i) by striking “consolidate, discontinue,” and inserting “discontinue”; and

(ii) by inserting after “reduce the staffing level” the following: “below the optimal staffing level determined in the most recent Resource Allocation Model required by section 301(h) of the Customs Procedural Reform and Simplification Act of 1978 (19 U.S.C. 2075(h))”; and

(B) in paragraph (2), by inserting “, National Account Managers” after “Financial Systems Specialists”; and

(2) by adding at the end the following:

“(d) AUTHORITY TO CONSOLIDATE, MODIFY, OR REORGANIZE CUSTOMS REVENUE FUNCTIONS.—

“(1) IN GENERAL.—The Commissioner of U.S. Customs and Border Protection may, subject to subsection (b), consolidate, modify, or reorganize customs revenue functions delegated to the Commissioner under subsection (a), including by adding such functions to existing positions or establishing new or modifying existing job series, grades, titles, or classifications for personnel, and associated support staff, performing such functions.

“(2) POSITION CLASSIFICATION STANDARDS.—At the request of the Commissioner, the Director of the Office of Personnel Management shall establish new position classification standards for any new positions established by the Commissioner under paragraph (1).”

(b) TECHNICAL CORRECTION.—Section 412(a)(1) of the Homeland Security Act of 2002 (6 U.S.C. 212(a)(1)) is amended by striking “403(a)(1)” and inserting “403(1)”.

SA 1997. Mr. WYDEN submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science

Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title III of division C, add the following:

SEC. 3314. PREVENTING IMPORTATION OF SEAFOOD AND SEAFOOD PRODUCTS HARVESTED OR PRODUCED USING FORCED LABOR.

(a) DEFINITIONS.—In this section:

(1) CHILD LABOR.—The term “child labor” has the meaning given the term “worst forms of child labor” in section 507 of the Trade Act of 1974 (22 U.S.C. 2467).

(2) FORCED LABOR.—The term “forced labor” has the meaning given that term in section 307 of the Tariff Act of 1930 (19 U.S.C. 1307).

(3) HUMAN TRAFFICKING.—The term “human trafficking” has the meaning given the term “severe forms of trafficking in persons” in section 103 of the Trafficking Victims Protection Act of 2000 (22 U.S.C. 7102).

(4) SEAFOOD.—The term “seafood” means fish, shellfish, processed fish, fish meal, shellfish products, and all other forms of marine animal and plant life other than marine mammals and birds.

(5) SECRETARY.—The term “Secretary” means the Secretary of Commerce, acting through the Administrator of the National Oceanic and Atmospheric Administration.

(b) FORCED LABOR IN FISHING.—

(1) RULEMAKING.—Not later than one year after the date of the enactment of this Act, the Commissioner of U.S. Customs and Border Protection, in coordination with the Secretary, shall issue regulations regarding the verification of seafood imports to ensure that no seafood or seafood product harvested or produced using forced labor is entered into the United States in violation of section 307 of the Tariff Act of 1930 (19 U.S.C. 1307).

(2) STRATEGY.—The Commissioner of U.S. Customs and Border Protection, in coordination with the Secretary and the Secretary of the department in which the Coast Guard is operating, shall—

(A) develop a strategy for using data collected under Seafood Import Monitoring Program to identify seafood imports at risk of being harvested or produced using forced labor; and

(B) publish information regarding the strategy developed under subparagraph (A) on the website of U.S. Customs and Border Protection.

(c) INTERNATIONAL ENGAGEMENT.—The United States Trade Representative, in coordination with the Secretary of Commerce, shall engage with interested countries regarding the development of compatible and effective seafood tracking and sustainability plans in order to—

(1) identify best practices;

(2) coordinate regarding data sharing;

(3) reduce barriers to trade in fairly grown or harvested fish; and

(4) end the trade in products that—

(A) are harvested or produced using illegal, unregulated, or unreported fishing, human trafficking, or forced labor; or

(B) pose a risk of fraud.

SA 1998. Mr. GRASSLEY (for himself and Mr. WHITEHOUSE) submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and

Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the end of title III of division B, add the following:

SEC. 2309. IMMIGRATION CONSEQUENCES OF TRADE SECRET THEFT AND ECONOMIC ESPIONAGE.

(a) **SHORT TITLE.**—This section may be cited as the “Stop Theft of Intellectual Property Act of 2021”.

(b) **IN GENERAL.**—

(1) **INADMISSIBILITY.**—Section 212(a)(3)(A) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(A)) is amended to read as follows:

“(3) **SECURITY AND RELATED GROUNDS.**—

“(A) **IN GENERAL.**—Any alien who a consular officer, the Secretary of Homeland Security, or the Attorney General knows, or has reasonable ground to believe, seeks to enter the United States to engage solely, principally, or incidentally in—

“(i) any activity to violate any law of the United States relating to espionage or sabotage;

“(ii) any activity to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information;

“(iii) any activity to violate any law of the United States or of any State relating to the theft or misappropriation of trade secrets or economic espionage;

“(iv) any other unlawful activity; or

“(v) any activity, a purpose of which is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means, is inadmissible.”.

(2) **DEPORTABILITY.**—Section 237(a)(4)(A) of the Immigration and Nationality Act (8 U.S.C. 1227(a)(4)(A)) is amended to read as follows:

“(A) **IN GENERAL.**—Any alien who has engaged, is engaged, or at any time after admission, engages in—

“(i) any activity to violate any law of the United States relating to espionage or sabotage;

“(ii) any activity to violate or evade any law prohibiting the export from the United States of goods, technology, or sensitive information;

“(iii) any activity to violate any law of the United States or of any State relating to the theft or misappropriation of trade secrets or economic espionage;

“(iv) any other criminal activity that endangers public safety or national security; or

“(v) any activity, a purpose of which is the opposition to, or the control or overthrow of, the Government of the United States by force, violence, or other unlawful means, is deportable.”.

(c) **ANNUAL REPORT OF INADMISSIBLE AND DEPORTABLE FOREIGN NATIONALS.**—Not later than 180 days after the date of the enactment of this Act, and annually thereafter, the Secretary of State, in cooperation with the Secretary of Homeland Security and the Attorney General, shall submit a report to the Chair and Ranking Member of the Committee on the Judiciary of the Senate and of the Committee on the Judiciary of the House of Representatives that identifies—

(1) the nationality and visa admission category of each of the foreign nationals who was determined, during the reporting period,

to be inadmissible under clause (ii) or (iii) of section 212(a)(3)(A) of the Immigration and Nationality Act, as amended by subsection (b)(1), or deportable pursuant to clause (ii) or (iii) of section 237(a)(4)(A) of such Act, as amended by subsection (b)(2); and

(2) the research institutions, private sector companies or other entities, United States Government agencies, and taxpayer-funded organizations with which such foreign nationals were associated.

SA 1999. Mr. KING (for himself and Mr. SASSE) submitted an amendment intended to be proposed to amendment SA 1502 proposed by Mr. SCHUMER to the bill S. 1260, to establish a new Directorate for Technology and Innovation in the National Science Foundation, to establish a regional technology hub program, to require a strategy and report on economic security, science, research, innovation, manufacturing, and job creation, to establish a critical supply chain resiliency program, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

Subtitle C—Cyber and Technology Diplomacy
SEC. 4271. SHORT TITLE.

This subtitle may be cited as the “Cyber Diplomacy Act of 2021”.

SEC. 4272. FINDINGS.

Congress makes the following findings:

(1) The stated goal of the United States International Strategy for Cyberspace, launched on May 16, 2011, is to “work internationally to promote an open, interoperable, secure, and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation ... in which norms of responsible behavior guide states’ actions, sustain partnerships, and support the rule of law in cyberspace”.

(2) In its June 24, 2013, report, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (referred to in this section as “GGE”), established by the United Nations General Assembly, concluded that “State sovereignty and the international norms and principles that flow from it apply to States’ conduct of ICT-related activities and to their jurisdiction over ICT infrastructure with their territory”.

(3) In January 2015, China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan proposed a troubling international code of conduct for information security, which could be used as a pretext for restricting political dissent, and includes “curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds”.

(4) In its July 22, 2015, consensus report, GGE found that “norms of responsible State behavior can reduce risks to international peace, security and stability”.

(5) On September 25, 2015, the United States and China announced a commitment that neither country’s government “will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors”.

(6) At the Antalya Summit on November 15 and 16, 2015, the Group of 20 Leaders’ communiqué—

(A) affirmed the applicability of international law to state behavior in cyberspace;

(B) called on states to refrain from cyber-enabled theft of intellectual property for commercial gain; and

(C) endorsed the view that all states should abide by norms of responsible behavior.

(7) The March 2016 Department of State International Cyberspace Policy Strategy noted that “the Department of State anticipates a continued increase and expansion of our cyber-focused diplomatic efforts for the foreseeable future”.

(8) On December 1, 2016, the Commission on Enhancing National Cybersecurity, which was established within the Department of Commerce by Executive Order No. 13718 (81 Fed. Reg. 7441), recommended that “the President should appoint an Ambassador for Cybersecurity to lead U.S. engagement with the international community on cybersecurity strategies, standards, and practices”.

(9) On April 11, 2017, the 2017 Group of 7 Declaration on Responsible States Behavior in Cyberspace—

(A) recognized “the urgent necessity of increased international cooperation to promote security and stability in cyberspace”;

(B) expressed commitment to “promoting a strategic framework for conflict prevention, cooperation and stability in cyberspace, consisting of the recognition of the applicability of existing international law to State behavior in cyberspace, the promotion of voluntary, non-binding norms of responsible State behavior during peacetime, and the development and the implementation of practical cyber confidence building measures (CBMs) between States”; and

(C) reaffirmed that “the same rights that people have offline must also be protected online”.

(10) In testimony before the Select Committee on Intelligence of the Senate on May 11, 2017, Director of National Intelligence Daniel R. Coats identified 6 cyber threat actors, including—

(A) Russia, for “efforts to influence the 2016 U.S. election”;

(B) China, for “actively targeting the U.S. Government, its allies, and U.S. companies for cyber espionage”;

(C) Iran, for “leverag[ing] cyber espionage, propaganda, and attacks to support its security priorities, influence events and foreign perceptions, and counter threats”;

(D) North Korea, for “previously conduct[ing] cyber-attacks against U.S. commercial entities—specifically, Sony Pictures Entertainment in 2014”;

(E) terrorists, who “use the Internet to organize, recruit, spread propaganda, raise funds, collect intelligence, inspire action by followers, and coordinate operations”; and

(F) criminals, who “are also developing and using sophisticated cyber tools for a variety of purposes including theft, extortion, and facilitation of other criminal activities”.

(11) Information and communication technologies are among a broader set of critical and emerging technologies that underpin United States national security and economic prosperity. The 2017 National Security Strategy noted the central importance of “emerging technologies . . . such as data science, encryption, autonomous technologies, gene editing, new materials, nanotechnology, advanced computing technologies, and artificial intelligence.”.

(12) The 21st century will increasingly be defined by economic and military competition rooted in technological advances. Leaders in adopting critical and emerging technologies, and those who shape the use of such technologies, will garner economic, military, and political strength for decades.